TUTTO QUELLO CHE GLI ALTRI NON OSANO DIRTI

NO PUBBLICITÀ
SOLO INFORMAZIONE E ARTICOLI
2,00 €

n.143
www.hackerjournal.it

HACKER JOURNAL



PROFESSIONE TRUFFATORE

La *RETE*, il paradiso degli *IMBROGLIONI*

LE 10 REGOLE D'ORO DELLA SICUREZZA

JAVA MOBILE

RIPROGRAMMATI il cellulare

LINUX

Crea e gestisci le tue *VIRTUALBOX*

IL PERICOLO CHIAMA AL TELEFONO

Tutti i *TRUCCHI* degli hacker per *INTERCETTARE LE TUE CHIAMATE*

Anno 8 – N.143
25 Gennaio / 7 Febbraio 2008

Editore (sede legale):
WLF Publishing S.r.l.
via Donatello 71
00196 Roma
Fax 063214606

Printing:
Roto 2000

Distributore:
M-DIS Distributore SPA
via Cazzaniga 2 - 20132 Milano

Copertina: Daniele Festa

HACKER JOURNAL
Pubblicazione quattordicinale registrata
al Tribunale di Milano
il 27/10/03 con il numero 601.

Una copia 2,00 euro

Direttore Responsabile:
Teresa Carsaniga

hack·er (hăk'∂r)
"Persona che si diverte ad esplorare i dettagli dei sistemi di programmazione e come espandere le loro capacità, a differenza di molti utenti, che preferiscono imparare solamente il minimo necessario."

editoriale



Auguri.it



Era il dicembre del 1987 quando nacque CNR.it, il primo sito internet a utilizzare il .it, tanta acqua è passata sotto i ponti e attraverso i modem... Si trattava di una scommessa allora e molti di noi non sapevano manco cosa fosse la rete, avevamo visto WarGames, il primo film che mi ricordi con una massiccia presenza di tecnologia di rete (ovvio che parliamo di cose un po' diverse da quelle che utilizziamo oggi). Oggi i siti che utilizzano il .it sono circa un milione e mezzo, un bella crescita che ha registrato accelerazioni e battute di arresto ma che ha portato a queste cifre. La spinta maggiore è stata a partire dal 2000 quando realmente si è iniziato a pensare che la rete poteva essere una risorsa da sfruttare anche in Italia (come sempre illuminati). Sicuramente i prossimi anni porteranno ad un ulteriore aumento di questi siti e speriamo ardentemente anche ad un miglioramento della qualità degli stessi, ma si sa, non si può avere tutto dalla vita. Per ora quindi tanti auguri .it e altri milel di questi giorni.



HACKER JOURNAL: INTASATE LE NOSTRE CASELLE

Diteci cosa ne pensate di HJ, siamo tutti raggiungibili via e-mail, tramite lettera o messo a cavallo... Vogliamo sapere se siete contenti, critici, incazzati o qualunque altra cosa! Appena possiamo rispondiamo a tutti, scrivete!

redazione@hackerjournal.it

Voliamo in Cina

:: Hacker in picchiata sul Boeing 787

Quando pensiamo di averle viste tutte salta fuori qualche spiritosone che ci fa immediatamente ricredere e rincuorare se pensiamo al nostro firewall non aggiornato o a quello scanning antivirus che non facciamo da troppo tempo. Si presuppone che chi progetta un aereo sia molto preparato, fior di cervelli attorno ad un tavolo che parlano di impedenza,



CX, sistemi integrati e misure della toilette... Possibile che tra tutti i vervelloni presenti non ci sia un addetto alla sicurezza informatica??? Perché dovete sapere che sul nuovo progetto della famosa azienda aeronautica, il Boeing 787 Dreamliner i sistemi di volo dell'apparecchio risultano in contatto con l'interfaccia che permette ai passeggeri di connettersi a internet...
Tutti possiamo ben immaginare cosa possa voler dire mettere questa possibilità a disposizione di un terrorista armato di conoscenze informatiche, altro che 11 settembre...

:: La cina contro YouTube

Dal 31 gennaio sarà perpetrato in Cina l'ennesimo affronto alla libertà di espressione e parola, tutto questo mentre gli occhi del mondo sono puntati sulla Repubblica Popolare in prossimità delle Olimpiadi. La vicenda sembra prendere spunto da un video postato poco tempo fa in rete dove la moglie di un popolare presentatore televisivo parla in maniera molto esplicita delle corna che il marito le mette regolarmente. A questo punto è partita la contro-offensiva statale portando al massimo livello la censura sui video in rete.



Solo i siti di proprietà statale potranno psotare video on-line con il limite di pubblicare immagini che non possano alterare l'ordine sociale del paese, contro la costituzione, contro l'unità nazionale, la sovranità, l'integrità territoriale e, ovviamente, quelli che divulgano segreti di stato, pregiudichino la sicurezza. Insomma, qualunque video postato potrebbe, se si volesse, rientrare in queste categorie e quindi portare all'oscuramento del sito dove si trova.



IL SESSO SBARAGLIA IN CINA

Secondo il quotidiano "China Daily" infatti la parola "stock" ha battuto la parola "sex" nella classifica di quelle più cercate dagli internauti cinesi nell'ultimo periodo. Lo studio è stato effettuato sulla versione cinese del motore di ricerca Google dove tra le prime sei parole più cercate dell'anno scorso, quattro sono legate al mondo della finanza. Tenendo conto che nel 2007 la borsa di Shangai ha avuto un rialzo medio del 97% i risultati delle ricerche cinesi non sono poi così tanto sorprendenti.

FIREFOX 3 IS COMING...



Firefox 3 è finalmente in dirittura d'arrivo! Mozilla ha pubblicato infatti la seconda e penultima beta di questa versione chiamata "Gran Paradiso" che dovrebbe portare oltre 900 migliorie in uno dei browsers alternativi (ad IE) più in voga del momento. Secondo gli sviluppatori le maggiori novità di questa versione saranno in buona parte dedicate ad incrementare velocità, stabilità, sicurezza, compatibilità ed ad aggiungere nuove funzionalità all'interfaccia grafica. La data di lancio ufficiale non è ancora stata fissata mentre in questi giorni (metà gennaio) dovrebbe essere rilasciata la terza ed ultima versione di test.

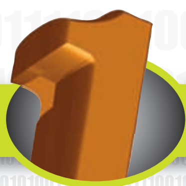
FALLA IN SKYPE!

È stata scoperta da uno sviluppatore una falla che colpiva da tempo il noto programma di VoIP "Skype". La falla riguarda una errata gestione del protocollo URI (Uniform Resource Identifier) che negli scorsi mesi aveva già dato problemi ad altri programmi come Firefox, Internet Explorer (versione 6 e 7) ed alcuni prodotti di casa McAfee. Grazie a questo bug un utente malintenzionato potrebbe indurre una persona a cliccare su indirizzi internet creati ad hoc per installare sul PC trojan, keylogger e altri dannosi malaware. Skype consiglia pertanto tutti gli utenti di aggiornare il proprio client alla versione 3.5



WIFI DANNOSO PER L'UOMO?

Una ricerca condotta da alcune università britanniche analizzerà gli effetti delle reti senza fili sull'organismo umano. Gli studi dureranno circa due anni e saranno commissionati dall'Agenzia per la protezione della salute britannica. Secondo il direttore di questo istituto attualmente non ci sono prove scientifiche che dimostrino come le reti senza fili (wifi/bluetooth) rappresentino




HOT NEWS

NASCE SIRIO IL VIDEOTELEFONO FISSO VOIP CHE PARLA LINUX!

Questo speciale telefono utilizza infatti una distribuzione mini di Linux per consentire di telefonare via VoIP senza dover utilizzare il pc e per gestire il collegamento wifi (disponibile come opzione). È possibile anche visualizzare alcuni contenuti del portale Virgilio direttamente nel display da 3,5" fornito assieme al telefono grazie al quale si può anche scaricare la rubrica del cellulare, vedere le ultime news o consultare le ultime previsioni meteo. 8) Trasformare IPOD Touch in IPhone... Impossibile? - L'ipod touch è stato da molti soprannominato come l'IPHONE senza telefono inquanto i due si assomigliano molto per il design ma non per le funzioni. Peccato però che da pochi giorni sembra possibile far diventare l'IPOD in un telefono grazie ad un software di Voice Over IP. Il programma prende il nome di SIP VoIP ed è sviluppato dal gruppo di "touchmods.net". Il software è un semplicissimo client VoIP (tipo Skype) che permette di effettuare chiamate quando è presente una connessione ad internet. Riguardo al microfono invece (non presente nelle caratteristiche standard dell' IPOD Touch) si consiglia di collegarne uno alla porta dock dello stesso lettore.



Rilasciato Wordpress 2.3.2

È stata rilasciata questa nuova versione di WordPress che va a correggere alcuni bug che permettono ad utenti remoti di visualizzare messaggi in attesa di pubblicazione. È consigliato quindi eseguire al più presto l'update per evitare spiacevoli inconvenienti o "tappare" il bug presente nel file "wp-includes\query.php" aggiungendo alla riga 37 il percorso assoluto relativo alla cartella "wp-admin" e, se usate il plugin per la cache ricordatevi di ripulirlo!

PREMIO MOST PIRATED

È uscita su "Wired News" come ogni anno, la speciale classifica dei film, delle canzoni e delle serie televisive più piratate del 2007. Questa classifica è stata stilata in base alle statistiche fornite da BigChampagne, una società specializzata nella rilevazione dell'audience di file nei circuiti peer-to-peer della rete eDonkey. Ecco qui chi vince il premio di "più piratato del 2007":

Canzoni:
1. Shop Boyz, "Party Like A Rock Star"
2. Akon, "I Wanna Luv U"
3. Sean Kingston, "Beautiful Girls"

Film:
1. Resident Evil: Extinction
2. Pirates of The Caribbean: At World's End
3. I Now Pronounce You Chuck & Larry

Serie Televisive:
1. "Heroes"
2. "Prison Break"
3. "Top Gear"

un rischio alla salute dell'uomo. Ricordiamo infatti che i segnali "in uscita" da router, antenne e computer sono molto deboli e si attestano generalmente intorno agli 0,1 watt. Ma perchè non fanno ricerche sulla pericolosità dell'uso del telefonino?



XBOX LIVE TORNA ALLA NORMALITÀ?

È questa la domanda che si chiedono molti giocatori dopo che negli scorsi giorni il servizio ha subito numerosi downtime e disfunzioni di vario genere. Secondo alcune voci, Microsoft sarebbe dell'idea di offrire un indennizzo agli utenti Gold di Xbox Live (che ricordiamo è un servizio a pagamento) regalando un abbonamento mensile. I problemi riscontrati nella maggior parte dei casi sono stati la difficoltà di accedere al servizio, seri problemi nella stabilità della rete, impossibilità nell'accedere e nel configurare il proprio account e altri problemi di vario genere. Iniziato proprio bene il 2008 per Microsoft vero?



A A A....

CRACKER CERCA LAVORO

Il programmatore del noto virus "Yamanner" che mesi fa aveva allertato 200 milioni di utenti di Yahoo!Mail, si è giustificato di averlo scritto dicendo: "Vengo dall'Iran e con Yamanner volevo solo trovare un lavoro nel campo della programmazione". Probabilmente è stato colpito da un precedente, nel 2004 infatti Sven Jaschan, creatore del worm Sasser aveva trovato lavoro, con la stessa tecnica, presso un'azienda dedicata alla sicurezza informatica. Ma anziché scrivere virus per far danni... non è più semplice mandare un curriculum come si fa usualmente?

I MAGGIORI INCIDENTI DEL 2007

È stata stilata pochi giorni fa una classifica chiamata "The major incidents on the internet in 2007. Questa lista redatta da Pingdom (società che offre servizi di monitoraggio degli uptime dei server) è inerente a tutti i peggiori downtime avvenuti nel corso dell'anno appena passato. Sul podio troviamo:

1)Skype: il peggiore downtime avvenuto per il numero di utenti coinvoli (oltre 10 milioni). Il problema è stato apparentemente dovuto ad un errato funzionamento di Windows Update.

2) RackSpace: tutto è avvenuto il 13 Novembre quando un camion ha letteralmente distrutto un trasformatore di energia, facendolo addirittura esplodere. Il calo di energia ha fatto entrare in funzione i sistemi di alimentazione, ma la sfortuna ha voluto che due generatori non abbiano funzionato correttamente, lasciando così "al buio" il datacenter per alcune ore.

3) Google Analytics: ha registrato un down di oltre 40 ore senza sapere a dire il vero quale fosse la causa.

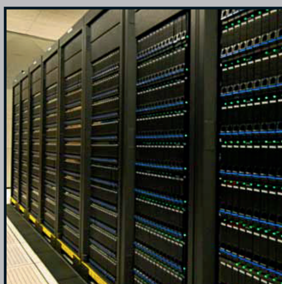
OPENMOKO, LO SMARTPHONE CON CORE LINUX



Già qualche mese fa aveva suscitato interesse nel mondo dei "Linux dipendenti" l'uscita dello smartphone Neo 1973, completamente open-source e basato su piattaforma Linux. È stato presentato in questi giorni il suo "fratello maggiore" chiamato NeoFreeRunner che, rispetto al modello precedente disporrà di un processore più potente (500Mhz), di connettività Wi-Fi (802.11b/g), e di connessione bluetooth. Come per il modello precedente il core sarà sempre una distribuzione Linux e sarà possibile acquistarne due versioni: la prima 850Mhz tri-band e la seconda a 900Mhz dual band. Maggiori informazioni su www.openmoko.com

SUPERCOMPUTER? IL MEGLIO SARÀ A LONDRA!

Il governo inglese ha infatti ufficialmente presentato l'High-End Computing Terascale Resources (HECToR), un nuovo centro di supercalcolo ospitato presso l'Università di Edimburgo che ospiterà presumibilmente il computer più veloce d'Europa. Il progetto costato oltre 150 milioni di euro è già stato avviato negli scorsi mesi ed in questo periodo ha aperto le porte agli istituti accademici e di ricerca britannici. L'hardware dedicato per la costruzione del sistema è costituito da un cluster di 60 server Cray XT4 Linux-based capaci di raggiungere una potenza di calcolo di quasi 60 teraFLOPS.



PRESO IL RE DELLO SPAMMER

È stato arrestato infatti Alan Ralsky un vero e proprio guru della posta indesiderata. L'uomo, attivo da molti anni, è stato accusato, assieme ad altri 10 suoi collaboratori, di aver violato le rigide leggi federali americane sullo spam. Su Ralsky gravano attualmente 41 capi diversi d'imputazione che gli potrebbero far scontare una pena di 20 anni di galera e 250 mila euro di multa per frode postale e telematica. Dimostrazione che alla fine c'è giustizia per tutti?



HOT NEWS

SUPER WIFI?

La nota casa di produzione di semiconduttori Marvell, presenterà durante il prossimo CES 2008 un nuovo chip WIFI che promette prestazioni molto interessanti. Attualmente la tecnologia più ottimizzata e veloce in questo settore è rappresentata dallo standard 802.11n (comunemente chiamato MIMO) che permette uno scambio di dati fino a 300Mbps. Il chip TopDog 11n-450 della Marvell permetterà di aumentare questa velocità fino a 450Mbps, e di aumentare il raggio di copertura del segnale del 160%. Questo risultato sembra sia stato raggiunto utilizzando 3 trasmettitori e 3 ricevitori direttamente impiantati nel core del chip. Le prestazioni dichiarate non sembrano affatto male... Staremo a vedere! Data di consegna: secondo trimestre 2008

GOOG1E.IT

CON RESPONSABILITÁ

È attivo da alcuni giorni il sito www.goog1e.it (con un uno al posto della lettera "l" per intenderci) che permette di effettuare ricerche con Google risparmiando energia elettrica. Vi chiederete come? "Goog1e.it" per effettuare le proprie ricerche su internet, fa risparmiare energia perchè lo schermo, durante la navigazione, è principalmente nero. Lo schermo del nostro pc che visualizza una pagina bianca consuma mediamente 74watt, contrariamente uno schermo che visualizza una pagina nera ne consuma mediamente 50. Questo sistema è valido sia per gli schermi CTR (a tubo catodico) che per quelli LCD (anche se in maniera minore). Perchè non provare allora? Impostate il sito come homepage del vostro browser e fate girare la voce!

UN PORTAFOTO UN PO' SPECIALE

Durante il congresso del CES di LasVegas la nota casa di prodotti tecnologici Parrot ha presentato un nuovo prodotto che ha suscitato molto interesse. È stato presentato infatti il DF7700, un "portafoto" un po speciale. Può infatti inviare e ricevere foto via MMS indipendentemente dal gestore di telefonia utilizzato e visualizzarle comodamente sullo "schermo" (grazie all'utilizzo con una comune scheda SIM). È dotato inoltre di una connessione USB e di un alloggiamento per MemoryCard SD. Il prezzo non è poi neanche tanto salato: 149 dollari ma al momento disponibile solo per gli utenti francesi



Cresce il numero di utenti Mac in rete

Secondo un monitoraggio condotto da Net Applications su 40.000 siti web nel mese di dicembre, gli utenti della nota azienda di Cupertino hanno avuto un aumento del 7% rispetto al mese precedente. Anche nel mese di novembre l'analisi aveva evidenziato un trend positivo che si era però fermato ad un aumento del 5%. Che sia l'anno del successo per Apple grazie anche all'uscita in larga scala del suo sistema operativo Leopard?

FURTO DI DOMINIO?

GRAZIE A GMAIL SI PUÒ

Uno dei più famosi designer di loghi e grafiche al mondo, David Airey si è infatti visto "fregare" il proprio dominio internet (http://www.davidairey.com/) da un cracker che ha furbescamente avuto accesso alla casella di posta di questo sfortunato grafico. Con l'accesso alla mail è infatti riuscito a modificare, tramite il pannello di gestione dei DNS del provider, il traffico diretto verso il dominio di David che è stato quindi inagibile per diversi giorni. L'attacker è riuscito ad avere accesso alle mail dell'utente sfruttando un baco di sicurezza nel sistema di Gmail. La webnews era infatti affetta da una falla che permetteva a siti maligni di effettuare attacchi di tipo Cross Site Request Forgery.



CONTRO GOOGLE ADSENSE

Secondo esperti di BitDefender è in giro per la rete un trojan che modifica le inserzioni pubblicitarie di casa Google sostituendole con pubblicità di altri siti. Il trojan che sfrutta un particolare tipo di "hijacking" va a modificare il file di host del computer infetto in modo tale da editare il server delle news di Google (page2.googlesyndication.com) con un altro indirizzo ip risedente su alcune macchine dell'est europa. Un nuovo modo per aumentare gli introiti della pubblicità di un sito?

Manuale di SOPRAVVIVENZA

Le dieci regole base per aver un PC a prova di scasso

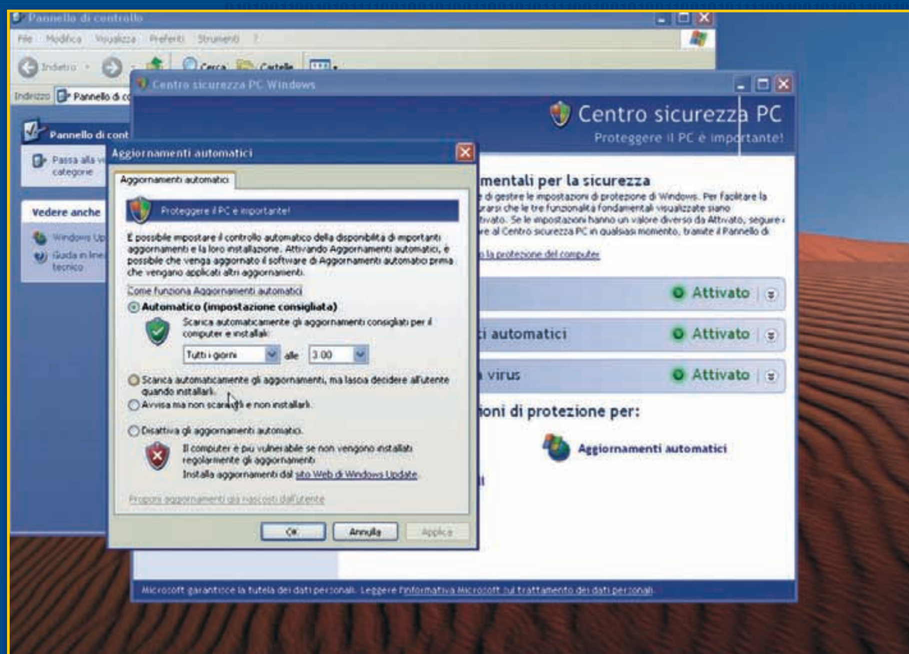
Antivirus e firewall sono strumenti indispensabili per proteggere il nostro PC. Oltre a questi, però, ci sono accorgimenti e buone abitudini che ci permettono di migliorare il livello di sicurezza del nostro computer. Basta seguire 10 preziose regole che ci consentono di eliminare i più comuni "buchi" di sicurezza".

1. Windows sempre aggiornato

Worm, trojan e spyware si diffondono utilizzando buchi di sicurezza del sistema operativo. Sempre più spesso, però, i punti deboli di Windows utilizzati per i loro attacchi sono già conosciuti nel momento in cui i virus fanno la loro comparsa e sono disponibili gli aggiornamenti che possono bloccarli. Cadono nella trappola, quindi, solo i PC che non sono in regola con gli aggiornamenti di Windows.



Per cercare di metter al sicuro il nostro computer e mantenerlo sempre aggiornato è sufficiente modificare le impostazioni dal Pannello di controllo alla voce Aggiornamenti automatici all'interno del Centro sicurezza PC. L'impostazione più affidabile è Automatico. Se giochiamo spesso e non vogliamo che l'installazione degli aggiornamenti rallenti il computer senza darci preavviso, possiamo invece scegliere la seconda voce che indica Scarica automaticamente gli aggiornamenti, ma lascia decidere all'utente quando installarli.



L'aggiornamento in automatico di Windows è la soluzione migliore per non farci trovare impreparati di fronte agli attacchi dei nuovi virus.

2. File sotto controllo

I virus si diffondono all'interno di file eseguibili. Ogni volta che ci troviamo di fronte a un file con estensione eseguibile, per esempio .EXE, .PIF o .CAB, dobbiamo quindi stare all'erta e, possibilmente, eseguire un controllo. Quando installiamo Windows, però, il sistema è impostato automaticamente in modo che i nomi dei file non comprendano l'estensione. Il file foto mare.jpg, quindi, comparirà solo come foto mare.

Per quanto comoda, si tratta di un'impostazione rischiosa che ci impedisce di riconoscere subito i file eseguibili. Spesso gli autori dei virus sfruttano l'impostazione per mascherare i file usando una doppia estensione, per esempio foto montagna.jpg.exe. Se il nostro computer fosse impostato per nascondere le estensioni dei file, il nome apparirebbe come foto montagna.jpg e rischieremmo di considerarlo un documento senza problemi.

3. Non rispondiamo allo spam

Nella nostra casella di posta elettronica arriva un'email pubblicitaria che riporta, al termine, una frase del tipo "Se non volete più ricevere messaggi scrivete a... . Non cadiamo nel tranello: si tratta di una strategia per verificare se l'indirizzo di posta elettronica è attivo e viene letto da qualcuno. Rispondendo al messaggio otterremo solo il risultato di essere inondati di email pubblicitarie.

4. Collegamenti pericolosi

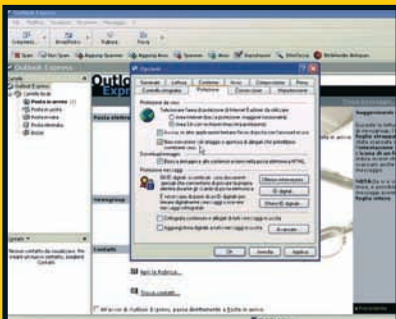


I collegamenti Web all'interno delle email hanno un aspetto innocuo e spesso può sembrarci che si riferiscano a siti Internet che conosciamo e consideriamo affidabili. Non sempre, però, il loro aspetto corrisponde al vero indirizzo a cui fanno riferimento. Nei messaggi di phishing, per esempio, i truffatori cercano di dirottarci verso siti simili a quelli della nostra banca su Internet per rubare i dati di accesso al conto corrente.

Il collegamento sembra identico a quello originale, ma se facciamo clic su di esso verremo indirizzati a una pagina Web completamente diversa,

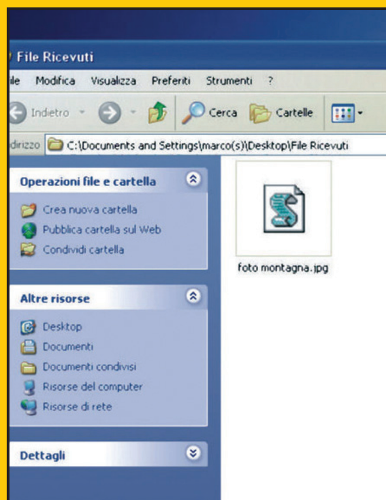
ALLEGATI BLOCCATI

Alcuni programmi di posta elettronica come Outlook e Outlook Express sono impostati per impedire il salvataggio e l'apertura di allegati pericolosi, tra cui i formati EXE. L'impostazione può essere modificata, ma è preferibile mantenerla. Per inviare e ricevere questo tipo di file possiamo usare la funzione Cartella compressa e convertire i file in formato ZIP prima di inviarli.



GUARDIAMO L'ICONA

Le impostazioni predefinite di Windows nascondono l'estensione dei file e questo può trarci in inganno. Il file in formato VBS infatti potrebbe contenere un virus, ma il sistema nasconde parte del nome. A tradire la vera natura del file è l'icona, che corrisponde a quella usata per i file di questo tipo. Anche se permette di smascherare l'inganno nella maggior parte dei casi, controllare il tipo di icona non è un metodo del tutto affidabile: il creatore del file può modificare facilmente l'impostazione e fare in modo che l'icona visualizzata sia diversa.



che ha solo l'aspetto del vero sito. In altri casi, invece, la pagina contiene virus o altri software pericolosi.
Per evitare la trappola è sufficiente collocare la freccia del mouse per qualche istante sul collegamento: apparirà il vero indirizzo Internet a cui "punta" il collegamento.

5. Attenzione al registro

I programmi spyware si installano sul nostro computer e modificano il registro di sistema per avviarsi ogni volta che accendiamo il PC. Per tenerli sotto controllo possiamo scegliere un programma antivirus che controlli in tempo reale tutte le modifiche al registro di Windows.
In alternativa, possiamo controllare manualmente l'elenco delle applicazioni che il sistema operativo avvia automaticamente. Se troviamo una voce sospetta è il caso di procurarci un programma antispyware e controllare il computer.

Una buona soluzione in questo caso è il programma Ad-Aware SE Personal, www.lavasoft.de. La versione di prova non sfrutta il sistema di protezione in tempo reale, ma è comunque in grado di rilevare ed eliminare gli spyware.

6. Orecchie aperte contro i dialer

Se usiamo una connessione a 56K, corriamo il rischio di rimanere vittime dei dialer, i programmi che modificano le impostazioni di connessione dirottandoci su numeri esteri o a pagamento. Un prezioso accorgimento, da tenere sempre presente per evitare brutte sorprese nella bolletta telefonica, è quello di impostare il modem in modo che la composizione del numero telefonico sia compiuta attraverso l'altoparlante del PC.

L'impostazione è possibile con la maggior parte dei modem e ci permette di accorgerci subito se il numero in composizione è cambiato.

7. Togliamo i privilegi

Windows XP permette di creare più Account a cui corrispondono i diversi utilizzatori del computer. La funzione permette di memorizzare le proprie impostazioni personalizzate e offre la possibilità di limitare i poteri degli account, escludendo i privilegi di amministratore.

Questi ultimi sono necessari per modificare le impostazioni di Windows e installare, eliminare o modificare i programmi. La funzione, però, può essere usata anche per garantire una maggiore sicurezza.
Per installarsi sul computer, infatti, molti virus e spyware devono avere accesso alle impostazioni del sistema. Lavorando con un Account di Windows XP che non abbia i privilegi di amministratore, la loro azione viene immediatamente bloccata.

8. Evitiamo i formati a rischio

I Macro Virus sono una particolare specie di virus che sfruttano le istruzioni Macro di Office. Queste ultime sono state pensate per inserire funzioni automatiche e scorciatoie all'interno dei documenti, ma nelle mani di un pirata informatico possono trasformarsi in uno strumento micidiale, in grado di mettere ko il nostro computer. Possiamo ridurre il rischio utilizzando dei formati diversi da quelli predefiniti, sostituendo per esempio i file



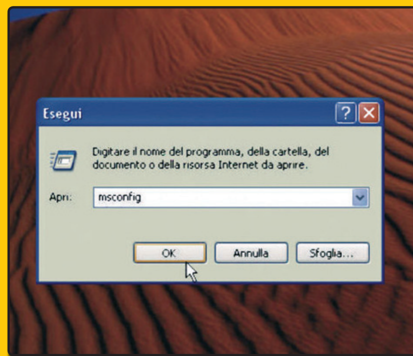
DOC con il formato RTF, che non contengono macro. Se usiamo il nuovo Office 2007, invece, tutti i programmi sono già impostati in modo da usare un formato che impedisce l'uso delle istruzioni Macro.

9. La prima connessione al Web

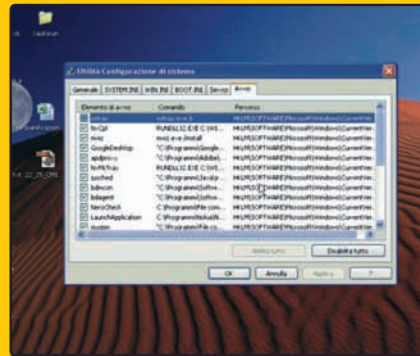
Formattare periodicamente il disco fisso e reinstallare Windows è una buona abitudine: consente di avere a disposizione un sistema pulito e un computer sempre efficiente. Quando eseguiamo questa operazione, però, dobbiamo ricordarci che il nostro PC perde tutti gli aggiornamenti di sicurezza che abbiamo installato nei mesi precedenti e potrebbe essere esposto agli attacchi via Web. Un PC equipaggiato con Windows XP senza il Service Pack 2, per esempio, viene insidiato dopo soli pochi minuti di connessione a Internet senza avere neanche il tempo di scaricare gli aggiornamenti più importanti.
Per evitare tutto ciò è importante seguire una procedura rigorosa prima di effettuare il collegamento alla Rete. Installiamo per prima cosa il Service Pack 2 di Windows XP tramite CD. In seguito, installiamo il programma antivirus e il firewall. Solo ora siamo pronti per collegarci al Web e avviare immediatamente Windows Update per scaricare tutti gli aggiornamenti di sicurezza.

ESTENSIONI SEMPRE VISIBILI

Windows è impostato per nascondere automaticamente l'estensione dei file. Disattivare questa funzione ci permette di individuare più facilmente i file che potrebbero contenere virus e spyware. Per farlo bastano pochi clic del mouse.



Apriamo una qualsiasi cartella di Windows, per esempio la cartella Documenti, e facciamo clic sulla voce Opzioni che troviamo all'interno del menu Strumenti in alto.

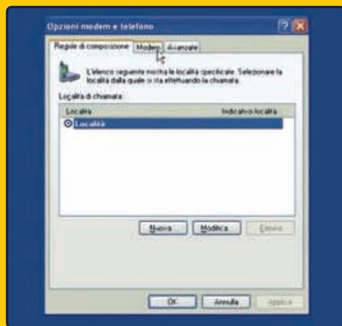


Facciamo clic sull'etichetta Visualizzazione e scorriamo l'elenco fino a identificare la voce Nascondi le estensioni per i tipi di file conosciuti. Togliamo il segno di spunta per disattivare la funzione e facciamo clic su OK.

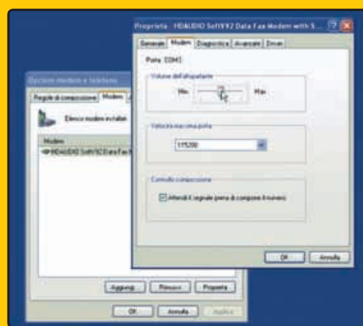
10. Antivirus sempre aggiornato

Equipaggiare il computer con un programma antivirus è indispensabile. Il nostro compito, però, non si esaurisce qui. Anche il miglior programma antivirus, infatti, è efficace solo se viene costantemente aggiornato.
Oltre le modifiche al software e al motore di scansione, l'aggiornamento installa le firme, ovvero i dati che permettono di identificare i nuovi virus che sono stati rilevati su Internet. Usare gli aggiornamenti manuali e affidarci solo alla nostra memoria è sempre una pessima idea: è meglio regolare le impostazioni del nostro antivirus in modo che si aggiorni automaticamente con una buona frequenza,al massimo ogni duegiorni.

DIAMO VOCE AL MODEM



Facciamo clic sul pulsante Start e scegliamo Pannello di controllo. Facciamo doppio clic su Opzioni modem e telefono. Nella nuova finestra che si apre selezioniamo con un clic del mouse la scheda Modem.



Qui troviamo un elenco dei modem installati. Selezioniamo quello che ci interessa e facciamo clic su Proprietà. Nella finestra selezioniamo la scheda Modem e trasciniamo con il mouse l'indicatore per regolare il volume in modo che la fase di composizione si possa sentire.

PROFESSIONE

TRUFFATORE DIGITALE

Internet è divenuta il nuovo terreno di caccia degli imbroglioni: ci sono soldi facili a volontà e tanti polli da spennare. Gruppi di pirati si sono organizzati per conquistare il territorio



Non si può negare che i truffatori siano fantasiosi quando si tratta di rubare denaro, sottrarre identità o mettere le mani su dati da rivendere. Le truffe sono molteplici e sempre più complesse. Ecco le tipologie principali.

:: Truffa 419

Vecchia come il mondo, questa truffa è risorta a nuova vita con l'avvento del digitale e di Internet. La truffa 419, nota anche come truffa nigeriana, va anche sotto il nome di "Fee Fraud" ed è finalizzata a sottrarre quattrini ai navigatori. Prima dell'avvento di Internet, i truffatori inviavano per posta una lettera in cui spiegavano di essere in possesso di vari milioni di dollari. Risiedendo in un paese africano, tuttavia, non potevano trasportare una simile quantità di denaro. La truffa non è cambiata molto con il Web e fa centinaia di vittime all'anno. L'obiettivo dei pirati è persuadere i navigatori a pagare le spese bancarie della transazione. Non pensiamo che nessuno abbocchi all'amo. Nel febbraio 2005 sei pirati sono stati arrestati dopo una truffa effettuata in Belgio via posta elettronica.

Nella trappola erano caduti un avvocato, un ufficiale giudiziario e un insegnante. I pirati avevano diffuso via Internet messaggi in cui dichiaravano che una somma di 9 milioni di dollari era stata nascosta nei locali di una società di sorveglianza. Per far scattare la trappola, i pirati invitavano le vittime ad andare a vedere di persona il denaro nascosto in alcune valigie nella sede dell'azienda di sorveglianza in questione. Lo scopo era quello di far pagare ai "gonzi" il costo del deposito, 12.500 euro, per riturare la valanga di denaro. Pochi giorni dopo l'incontro, il falso sorvegliante minacciava di rivelare tutto alla polizia… chiedendo 50.000 euro in cambio del suo silenzio. E questo è il meno: naturalmente, le banconote all'interno delle valigie erano false!



▲ *Un falso sito che intercetta i dati di coloro che richiedono una Green Card.*

:: Green Card

Molti navigatori di Internet sognano l'Eldorado americano. Per toccare con mano lo Zio Sam esiste una sola possibilità: la Carta Verde

o Green Card. Questo celebre documento permette di risiedere a tempo indeterminato negli Stati Uniti. Si tratta di una carta di identità ufficiale rilasciata dal Dipartimento di Stato americano, che permette ai cittadini non americani di trasferirsi e di lavorare legalmente negli Stati Uniti. Questa famosa carta suscita una certa cupidigia e alcuni truffatori hanno capito quanto possa essere redditizio trarre in inganno coloro che la richiedono.

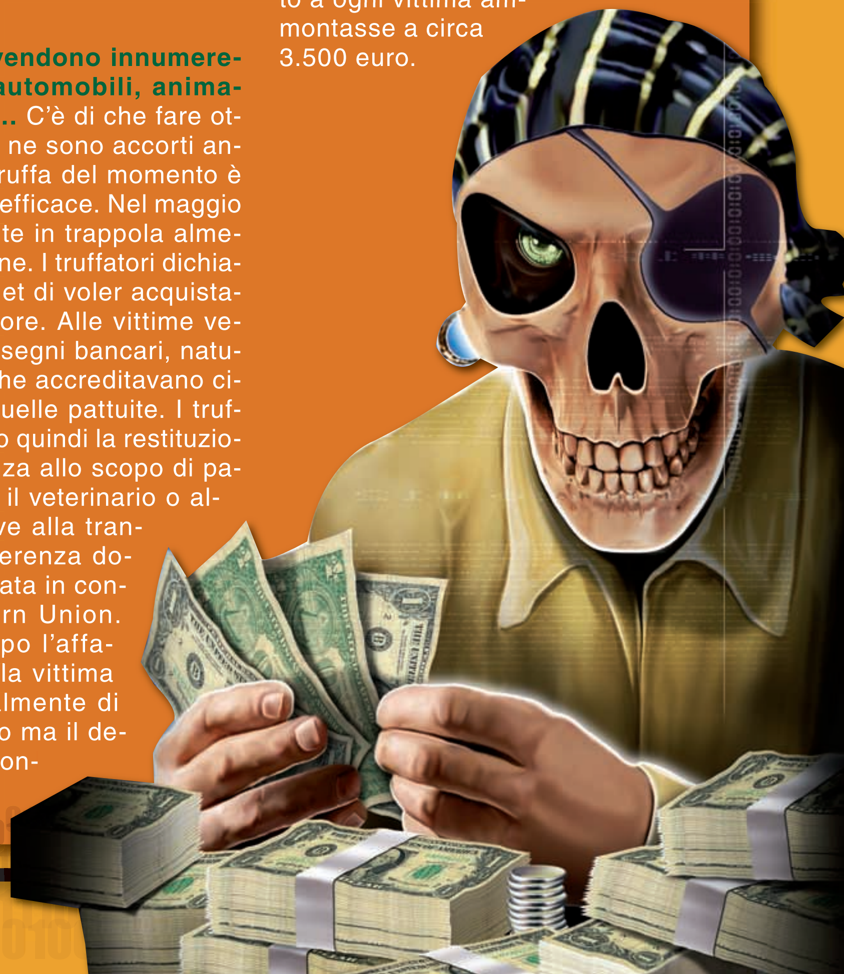
Basta una semplice ricerca su Google per farsi un'idea della situazione. Occorre ricordare che Carta Verde può essere richiesta gratuitamente. La concessione dipende da una sorta di "lotteria" gestita in esclusiva dalle ambasciate americane. I truffatori giocano però sulla disinformazione da parte dei navigatori che richiedono la carta.

I pirati mettono quindi on-line falsi siti che annunciano facilitazioni per l'ottenimento di una Green Card; favori fasulli che si pagano a caro prezzo. "Non va presentato alcun documento." - conferma l'ambasciata USA - "Solo le ambasciate sono autorizzate a ricevere le domande". Truffe analoghe esistono anche in Europa. Un 34enne greco è stato arrestato qualche tempo fa per una truffa su Internet. Offriva delle "facilitazioni" per posti di lavoro nell'ambito della pubblica amministrazione. I suoi "favori" erano in vendita a prezzi compresi tra i 500 e i 2000 euro.

Una pagina on-line con un falso codec video che contiene un virus vero.

:: Venduto a 500, pagato 750

Su Internet si vendono innumerevoli prodotti: automobili, animali, gioielli, hi-fi... C'è di che fare ottimi affari ma se ne sono accorti anche i pirati. La truffa del momento è tremendamente efficace. Nel maggio 2005 sono cadute in trappola almeno 30.000 persone. I truffatori dichiaravano su Internet di voler acquistare oggetti di valore. Alle vittime venivano inviati assegni bancari, naturalmente falsi, che accreditavano cifre superiori a quelle pattuite. I truffatori chiedevano quindi la restituzione della differenza allo scopo di pagare la dogana, il veterinario o altre spese relative alla transazione. La differenza doveva essere inviata in contanti via Western Union. Pochi giorni dopo l'affare, la banca della vittima rifiutava puntualmente di pagare l'assegno ma il denaro inviato in contanti era ormai nelle tasche dei truffatori. La polizia calcola che il denaro "in più" sottratto a ogni vittima ammontasse a circa 3.500 euro.



Dietro queste affascinanti russe c'è una truffa on-line in agguato per gli uomini.))

:: Quella ragazza è un uomo

La grande novità di Internet è la possibilità di inventarsi una vita, una personalità. Molti dei nuovi pirati, a volte veri e propri schizofrenici, non esitano a tendere tranelli ai frequentatori delle chat in cerca d'amore. Louri, 34 anni, è originario degli Urali. Quest'uomo truffava i navigatori alla ricerca di una donna da sposare. Facendosi passare per varie fanciulle, Louri è riuscito a farsi dare non meno di 232.612 euro a scapoli americani, belgi, francesi e italiani. Il truffatore è stato condannato a un anno di prigione con la condizionale.

Ed ecco un altro tipo di truffa. Su forum e chat, i pirati si fanno passare per Mélanie, Justine o Chloé per attirare i navigatori voyeur. Adescato il cliente, il pirata, sotto le spoglie di una ragazza, gli propone di sbirciarla per un'ora, al prezzo di un euro, tramite la sua webcam. Per fare questo, il "pollo" deve indicare il numero della sua carta di credito. Naturalmente, queste informazioni serviranno a soddisfare tutti i desideri... del pirata!

RUSSIAN BUSINNES NETWORK

Il server Russian Business Network (RBN - rbnnetwork.com) sembra essere scomparso dalla rete da metà novembre. È la fine di un affare elettronico mafioso o semplicemente una scomparsa temporanea finalizzata a far sparire le tracce dei malviventi? Per la cronaca, RBN è un server con sede a San Pietroburgo, in Russia, specializzato nella fornitura di spazio Web ai pirati: si va dai programmi dannosi al phishing e ad altri file pericolosi, fino al warez e alla pedofilia. L'ultima apparizione conosciuta di RBN ha riguardato la massiccia diffusione di e-mail non richieste che contenevano file PDF infetti. Anche il virus Storm è partito da uno dei server di RBN. Praticamente tutti i sistemi indipendenti di RBN conosciuti (RBN-AS, SBT-AS, MICRONNET-AS, OINVEST-AS, AKIMON-AS, CONNCETCOM-AS e NEVSKCC-AS. CREDOLINK-ASN) sono recentemente scomparsi dalle tabelle che controllano il traffico su Internet. Questi professionisti della truffa, tuttavia, non sono affatto spariti. Pochi giorni dopo la scomparsa di RBN, un attacco ha colpito il sito di richieste e offerte di lavoro Monster.com. Si è trattato di un episodio di pirateria impressionante. Nel sito è stato scoperto un iframe pirata. Questo iframe, un grande classico da alcune settimane, indirizzava i navigatori verso un'altra pagina Web che conteneva un programma dannoso. Si trattava di un virus finalizzato alla sottrazione di dati dai sistemi infetti. Un attacco mirato e particolarmente ben preparato, rivolto contro le aziende che utilizzavano Monster per la ricerca di personale. Un dato interessante: una delle connessioni pirata rimandava a un server utilizzato dai russi di RBN in Australia (myrdns.com).

In memoria di NETSCAPE



La notizie è di quelle tristi ma sicura, Netscape smetterà di esistere dal 1 febbraio 2008

Non avevamo ancora finito di festeggiare l'uscita di Netscape 9 che su di noi si abbatte la tristezza di questa notizia per molti tragica... Il primo browser, in termini cronologici, ha deposto le armi contro i giganti Firefox, IE e compagnia bella. Il vecchietto, da molti amato e ancora utilizzato, smetterà definitivamente di essere sviluppato dal 1 febbraio 2008, come si può leggere nel sito del browser. È un peccato, non amiamo che un software muoia, mai, a prescindere dalla qualità stessa del software, inoltre Netscape è stato per molti di noi un amico fidato per lungo tempo. Purtroppo una quota di mercato pari a all'1% non giustifica ulteriori sviluppi, peccato anche alla luce della versione 9 (che oltretutto aveva ripreso il nome completo Netscape Navigator) un vero passo in avanti rispetto alla versione 8 (sviluppata all'esterno) e che aveva fatto storcere il naso a molti utenti. Siamo sicuri che sarà possibile scaricare ancora per molto il browser da vari e siti e quindi vi riportiamo qualche specifica dell'utlima release.





Il codice di base è quello di Firefox, per la precisione della versione 2.0.0.7 da cui eredita alcune funzioni come i Live Bookmark, il riavvio con il recupero dei tab aperti, la gestione dei feed RSS, l'architettura espandibile e altre ancora. Rispetto al precedente e molto discusso Netscape 8, sviluppato dalla Mercurial Comunications, la versione 9 abbandona il motore di rendering di IE per affidarsi alle capaci mani di Mozilla Gecko, orami affidabile e ben sviluppato. Altre funzioni interessanti sono la correzione automatica degli URL, il link pad, che permette di appuntarsi velocemente degli indirizzi che ci serviranno solo per poco, inoltre è possibile usale la sidecar come mini-browser per visualizzare dei link senza abbandonare la pagina principale aperta nel browser. Insomma un buon browser che però è destinato a vedere calare il sapario... ■

Tutti come MOGGI

È partito il processo Calciopoli, fondanto tutto sulle intercettazioni telefoniche scopriamo quali sono le tecnologie utilizzate per farle e come proteggerci dagli spioni

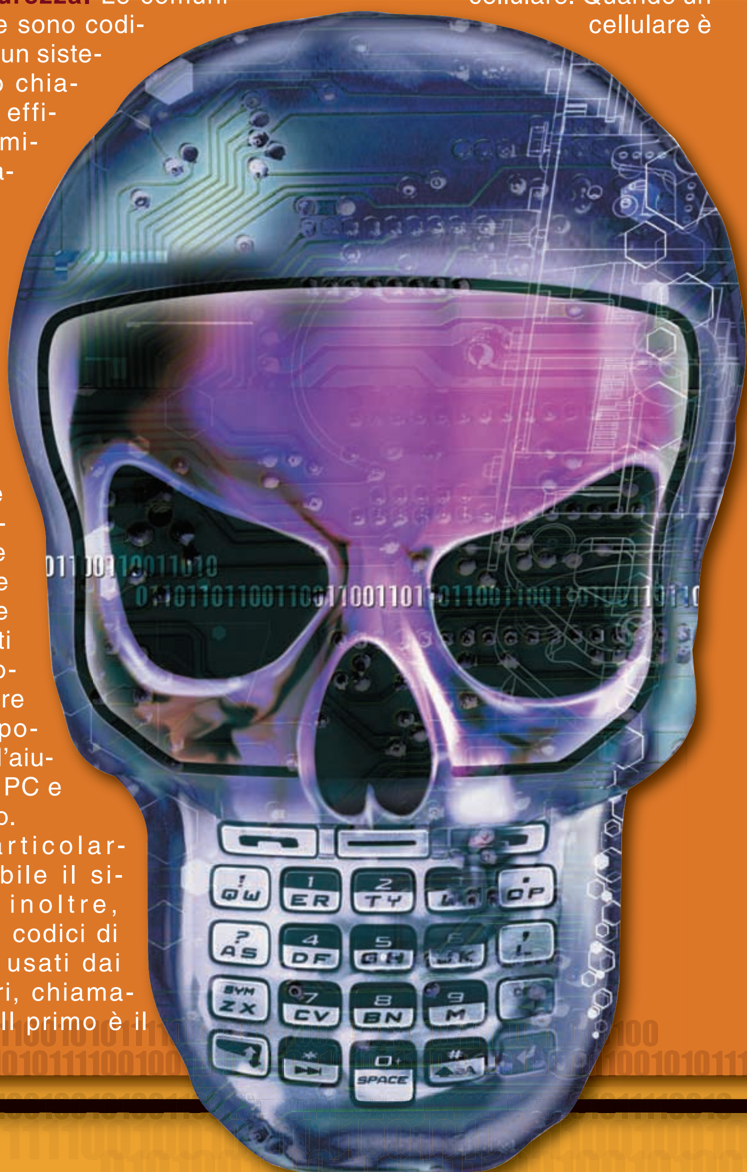
Il primo allarme è arrivato con le intercettazioni telefoniche di "calciopoli" e le inchieste sul mondo della finanza. Le roventi polemiche dei mesi seguenti lo hanno confermato: intercettare un telefono cellulare è fin troppo facile e per farlo non è necessario avere alle spalle poliziotti e magistrati.

CODIFCA SOFTWARE

L'acquisto di un cellulare con codifica crittografica hardware non è l'unica soluzione per cautelarsi dalle intercettazioni. È possibile, infatti, equipaggiare un telefono con un software in grado di proteggere le chiamate con la stessa efficacia. Tra i programmi troviamo per esempio GLK, la cui versione "base" offre garanzie di sicurezza, ma una scarsa compatibilità: può essere installato solo sul Nokia N70. Il funzionamento, inoltre, è piuttosto deludente: sul sito www.eebd.eu scopriamo che per parlare in "sicurezza" con un altro telefono dotato dello stesso software dovremo premere un pulsante sul telefono, come se stessimo usando un walkie-talkie. Per poter effettuare una chiamata "normale" è necessario passare alla versione Full Duplex, che vanta anche una maggiore compatibilità hardware.

:: Un sistema debole

Le caratteristiche della rete GSM, usata dalla maggior parte dei telefoni cellulari, offrono ben poche garanzie di sicurezza. Le comunicazioni sulla rete sono codificate attraverso un sistema crittografico chiamato A5, la cui efficacia è molto limitata. La crittografia, infatti, è stata pensata principalmente per evitare la cosiddetta clonazione delle schede, che qualche anno fa aveva causato grossi problemi con la rete ETACS. La crittografia A5, però, è ben poco efficace nella protezione dei dati scambiati e le conversazioni possono essere decodificate in pochi secondi con l'aiuto di un normale PC e il software adatto.
A rendere particolarmente vulnerabile il sistema GSM, inoltre, contribuiscono i codici di identificazione usati dai telefoni cellulari, chiamati IMSI e IMEI. Il primo è il codice che identifica le schede telefoniche, o SIM. Il secondo, invece, fa riferimento al telefono ed è riportato anche su un'etichetta che troviamo solitamente sotto la batteria del cellulare. Quando un cellulare è



COSA DICE LA LEGGE

Per la legge italiana, l'acquisto di dispositivi di sorveglianza, compresi i telefoni spia, è legale. L'avvocato Luca Sandri spiega però che "l'uso che se ne può fare è limitato dalle norme in tema di tutela della riservatezza e interferenze illecite nella vita privata. È possibile, quindi, usare detti dispositivi nella sfera privata, ad esempio per sorvegliare la nostra abitazione quando non ci siamo o per controllare a distanza i figli neonati. Qualsiasi uso che comporti la sorveglianza di terze persone, invece, è riservato esclusivamente agli ufficiali di Polizia Giudiziaria muniti di autorizzazione da parte dell'Autorità Giudiziaria e limitatamente ai casi di legge. Anche in questo caso, però, l'uso di strumenti per l'intercettazione diversi da quelli installati presso la Procura è permesso solo nel caso in cui questi ultimi non siano sufficienti o vi siano eccezionali ragioni d'urgenza".

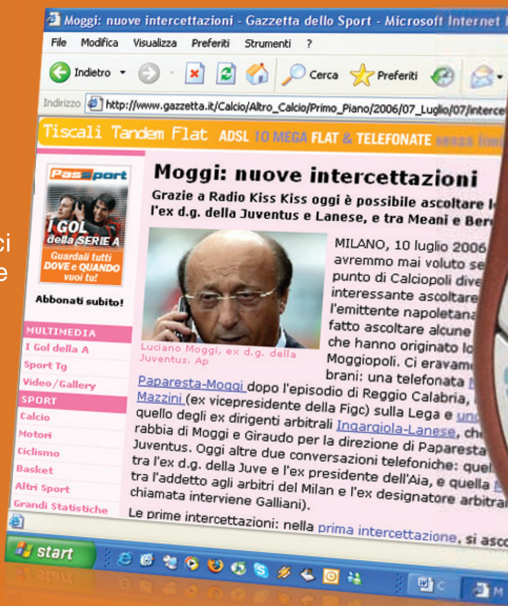




acceso e collegato alla rete, i codici permettono di identificare il telefono e la scheda senza margine di errore.

:: Spioni fai da te

L'intercettazione di un cellulare GSM può avvenire attraverso diversi metodi. Alcuni di questi richiedono la collaborazione degli operatori telefonici e sono quindi riservati a istituzioni, come la magistratura, che operano "alla luce del sole", seguendo rigorosamente le procedure previste dalla legge.
Altri metodi, però, possono essere utilizzati da chiunque abbia gli strumenti adatti e una buona conoscenza del sistema di comunicazione GSM. Il più diffuso è quello che sfrutta una forma di dirottamento delle comunicazioni e richiede l'uso di un





IL PREZZO DELLA RISERVATEZZA



Sull'onda delle vicende di cronaca, sono comparse decine di siti Internet e negozi che propongono telefoni cellulari "sicuri". In molti casi, però, le tecnologie utilizzate offrono ben poche garanzie o utilizzano tecniche che violano le leggi del nostro paese. Tra i produttori più "seri" e apprezzati del settore c'è l'italiana Caspertech, www.caspertech.com, che propone una linea di cellulari equipaggiati con un software crittografico estremamente potente. Regalarsi un "criptofonino" di questo livello, però, può costare fino a 2.700 euro IVA inclusa. Nel prezzo è comunque compreso un servizio di assistenza che prevede, pagando la sola installazione del software, la fornitura di un nuovo telefono in caso di guasto, furto o smarrimento.





dispositivo chiamato "Cattura IMSI". Si tratta, in pratica, di un dispositivo che trasmette in un'area limitata un segnale identico a quello delle stazioni cellulari.

Quando è attivo, funziona come "ponte" tra i cellulari che trasmettono nella zona e una vera stazione cellulare, alla quale il dispositivo re-indirizza il segnale per consentire la ricezione e l'invio di chiamate e messaggi. Quando giunge una richiesta di chiamata in partenza o in ricezione da parte del cellulare sotto sorveglianza, questo viene identificato attraverso il codice IMSI contenuto nella scheda SIM.

La chiamata in questione viene quindi re-indirizzata come le altre, ma il dispositivo invia una trasmissione parallela a una stazione d'ascolto pirata, che registra la conversazione.

:: Telefoni modificati

Il sistema del dirottamento consente di intercettare un cellulare senza nemmeno toccarlo, ma gli strumenti necessari per questo tipo di operazione sono molto costosi e difficili da usare. Se lo spione di turno ha la possibilità di mettere le mani sul telefono, invece, può ottenere lo stesso risultato utilizzando strumenti molto più "abbordabili". Su Internet troviamo numerosi siti che mettono a disposizione cellulari e accessori modificati in modo da registrare segretamente le conversazioni.

I cellulari-spia consentono l'intercettazione delle chiamate, degli SMS e la localizzazione geografica del cellulare. In alcuni casi, però, le modifiche permettono di andare oltre, trasformando il dispositivo in una "cimice" che consente di ascoltare tutto ciò che avviene nei paraggi. Alcuni siti, inoltre, propongono una funzione che permetterebbe di utilizzare i cellulari come microspie anche quando sono spenti, ma le stesse pagine Web avvertono che la vendita è riservata alle sole forze dell'ordine. Quali che siano le funzioni a disposizione, il prezzo di questi

Tra le "vittime" illustri delle intercettazioni telefoniche c'è anche l'attrice Anna Falchi. Poche settimane dopo la vicenda, la stessa Falchi ha scelto di prestare la propria immagine per pubblicizzare Enigma, un telefono cellulare a prova di intercettazioni.

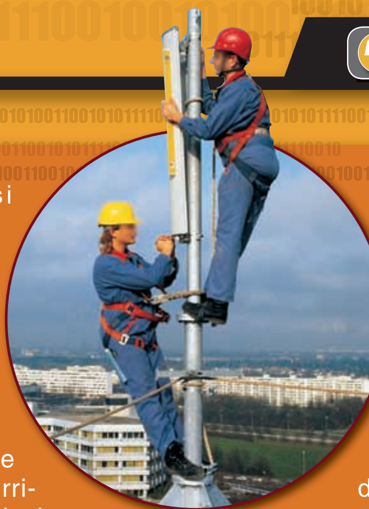
SPIA O VIRUS?

La soluzione più economica e alla portata di tutti per spiare un cellulare si chiama FlexiSpy, ed è un software la cui versione Light è in vendita su Internet a soli 50 euro. Si tratta di un programma compatibile con i sistemi Symbian che è in grado di registrare l'elenco delle chiamate effettuate e ricevute dal telefonino e tutti gli SMS che sono stati scambiati. Il programma si installa sul cellulare come qualsiasi altra applicazione e richiede una connessione GPRS attraverso la quale inviare i dati relativi alle chiamate e ai messaggi. Le informazioni raccolte in questo modo potranno essere visualizzate in qualsiasi momento attraverso una normale pagina Internet. La versione Pro del programma, della quale è disponibile un abbonamento annuale al prezzo di 150 euro, permette anche di usare il telefono come microfono per ascoltare tutto ciò che accade nell'area circostante il cellulare. Le caratteristiche di questo software hanno procurato qualche guaio alla società che lo produce, al punto che FlexiSpy è stato più volte indicato come un virus per cellulari. La definizione, per lo meno sotto un profilo squisitamente tecnico, è però sbagliata: il programma prevede infatti una procedura d'installazione chiaramente segnalata e deve essere opportunamente configurato.

"giocattoli" supera facilmente i 1.000 euro. Per alcuni modelli di cellulari sono disponibili anche software specifici che permettono di ottenere lo stesso risultato senza apportare alcuna modifica all'hardware del telefono.

:: Le contromisure

Se i sistemi di spionaggio sembrano aver conquistato un buon mercato, il vero "boom" di vendite si registra negli strumenti per la protezione dalle intercettazioni. A richiedere questo tipo di dispositivi sono uomini d'affari e personaggi famosi che temono di poter essere controllati. Le strategie per difendersi dagli spioni sono numerose. La più "casereccia" è il ricorso ai dispositivi in grado di alterare la voce per renderla irriconoscibile, ma non risolve tutti i problemi.
Anche se lo spione non può essere sicuro dell'identità di chi parla, potrà infatti sentire il contenuto della conversazione.
La contromisura più efficace consiste nell'uso dei cosiddetti "criptofonini", telefoni cellulari dotati di un sistema di protezione crittografico dei dati. Per conversare in modalità "sicura" con questi dispositivi è necessario, comunque, che il nostro interlocutore stia usando un telefono dello stesso tipo, in grado di utilizzare il medesimo sistema crittografico. Chi dovesse intercettare e registrare una conversazione protetta da crittografia, sentirebbe soltanto suoni e rumori incomprensibili.



Marco Schiaffino

INTERCETTAZIONE PIRATA

Il dispositivo "Cattura IMSI" emette un segnale simile alle stazioni cellulari per ingannare i telefoni nell'area e fare in modo che si colleghino ad esso, re-indirizzando tutti i segnali a una vera stazione cellulare per fare in modo che tutto funzioni normalmente. Quando identifica il telefono che vuole intercettare, avvia una trasmissione parallela verso una stazione di ascolto pirata.

Il browser SBOKKATO

Un'aggiunta stracarica di humor nero che trasforma l'elegante volpe di fuoco nello scaricatore di porto di Internet

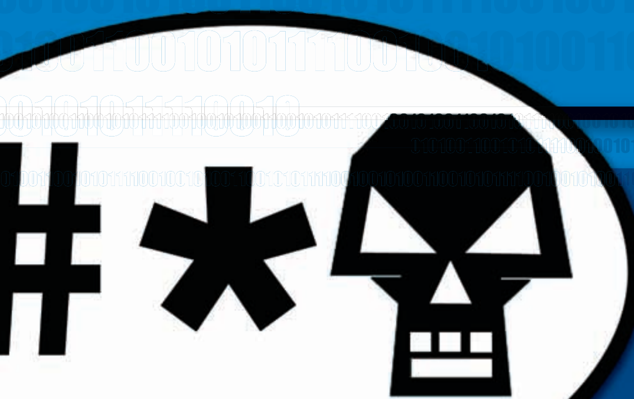
Uno dei motivi per cui Firefox si è conquistato un pubblico fedele e molto ampio tra gli utenti più esigenti e smanettoni è il suo sistema di estensioni. Da soli o in combinazione con altri script (come è il caso di Greasemonkey) i plugin per il programma della fondazione Mozilla permettono di fare di tutto o quasi, trasformando in browser in un server web, uno strumento di videoscrittura, un player audio ed altro ancora. Tra le invenzioni in assoluto più assurde c'è un'estensione molto particolare che risponde al nome Tourettes Machine (http://fffff.at/tourettes-machine/). Inutile, divertente e anche un po' offensiva è un'operazione artistica del laboratorio/collettivo F.A.T. (Free Art & Technology) che si "ispira" alla Sindrome di Tourette (http://it.wikipedia.org/wiki/Sindrome_di_Tourette), malattia che può causare spasmi, tic e far dire parole volgari in maniera incontrollata. L'aggiunta di Tourettes Machine a Firefox serve proprio a questo: a trasformare il browser open source in un qualcosa che genera parolacce e le infila senza alcuna pietà in tutti i testi che digitiamo. Forum, e-mail, ricerche: ovunque.



:: Come ***** si installa

Tourettes Machine, come tutte le estensioni per Firefox, è multipiattaforma e quindi funziona su Windows, Linux e Macintosh. Quando si installa, all'indirizzo http://fffff.at/tourettesmachineinstall/ ci ci viene però proposta una scelta.

Esistono due versioni del plugin, quella "moderate", che aggiunge insulti ogni tanto (dopo una media di 4 parole) oppure "extreme", che si scatena dopo



**** ogni *****
parola ***** che
**** scriviamo ******.

Dopo un click sulla versione che preferiamo e Firefox ci proporrà la

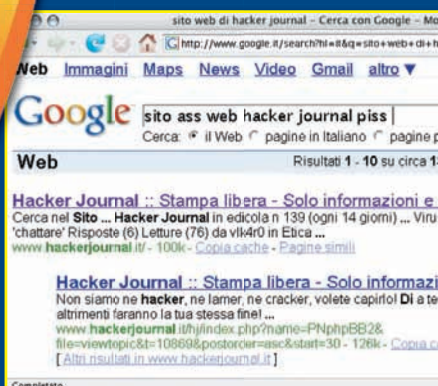
install tourettes machine moderate

install tourettes machine extreme

finestra per l'installazione e poi di riavviare per completare la procedura.

:: Parole in libertà

A questo punto in soli 7 KB Tourettes Machine è pronta e "helps with shit your spelling", tanto per usare il motto ufficiale. Mettiamola alla prova in una innocente ricerca e tra una parola e l'altra troveremo delle sorpresine. Attenzione a non dimenticarsi della presenza dell'estensione: se si è installata la versione "moderata" e considerato che su alcune finestre e form non funziona ci si può dimenticare di averla e poi rimanere di stucco, magari mentre scriviamo con Firefox un commento su un blog o in una sessione di Instant Messaging via browser.



:: Solo "curse words"?

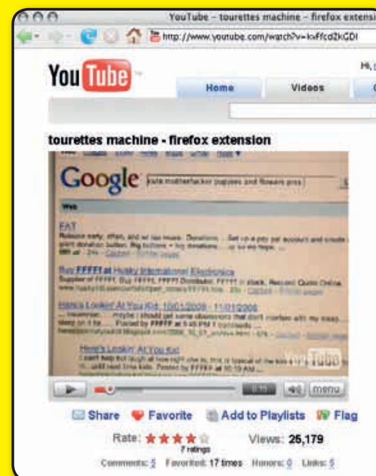
L'unico "limite" (se così si può dire) di Tourettes Machine è che i termini volgari sono in inglese. Chi volesse avere insulti nella propria lingua madre dovrà rimboccarsi le maniche e localizzarlo, grazie al codice sorgente che quelli di F.A.T. "gentilmente" ci forniscono sul loro sito internet (http://fffff.at/tourettesmachineinstall/src/) con istruzioni per la trasformazione in estensione

Nicola D'Agostino
www.nicoladagostino.net



IL VIDEO DIMOSTRATIVO

Per chi vuole vedere cosa riesce a combinare l'estensione su YouTube è disponibile un video (http://www.youtube.com/watch?v=kvFfcdZkGDI) in cui si mostra l'installazione di Tourettes Machine e poi la si ammira (?) all'opera su Google e nella stesura di un messaggio in GMail.



Un'ILLUSIONE da 150 dollari

Mentre Negroponte e altri pontificano su computer da 100 dollari per il terzo mondo, l'illustre sconosciuto Valdi Ivancic lo scorso luglio ha messo in vendita un discreto notebook a 150 dollari, spese di spedizione comprese. Peccato che non sia arrivato a nessuno

Correva lo scorso luglio quando la rete venne sconquassata da una notizia clamorosa: il sito www.madisoncelebrity.com proponeva al mondo un notebook per 150 dollari, poco più di 100 euro al cambio attuale. In molti non hanno esitato a dare la notizia come attendibile, tra i quali il peraltro affidabile affidabile Macynet (www.macitynet.it/macity/aA28984/index.shtml). D'altra parte, a una prima occhiata su quel sito, tuttora aperto anche se non accetta più prenotazioni per il notebook da saldo, sembrava tutto regolare. Il notebook non era dell'ultima generazione, cosa che avrebbe potuto insospettire visto il prezzo di vendita, ma era un onesto prodotto con processore Celeron M 370, schermo da 14 pollici, hard disk da 40 GN e 256 MB di memoria Ram. Il sistema operativo era Linux. Insomma, un'offerta in bilico tra il probabile e l'improbabile. Non un computer potentissimo, ma meglio di quello pensato da Negroponte per il terzo mondo. Ma a dare una luce di affidabilità al sito era soprattutto il fatto che la logistica dell'operazione era stata affidata a 2Checkout, una solida e onesta compagnia di distribuzione internazionale che si occupa di raccogliere i soldi e di spedire i prodotti che gli vengono affidati da centinaia di produttori. Se da una parte c'era una sconosciuta Madison Celebrity che faceva capo a un fumoso Valdi Ivancic (reperibile comunque in rete con un'infinità di recapiti), dall'altra c'era una società di distribuzione a prova di ogni sospetto.

:: I due fronti

Una settimana dopo l'annuncio ufficiale della raccolta delle prenotazioni per il notebook da 150 dollari, il popolo della rete era diviso in due fronti: chi riteneva valida l'offerta e chi la riteneva una truffa. I primi davano retta a quello che sosteneva Ivancic e cioè che quel prezzo era possibile grazie al fatto che sarebbe stati usati componenti obsoleti (vero) e che l'assemblaggio sarebbe stato fatto in Brasile (notizia mai confermata). Ed erano sicuri che non poteva essere una

truffa vista la nota serietà di 2Checkout (www.2checkout.com), che sin dall'inizio si dichiarava pronta a rimborsare i clienti se i prodotti non sarebbero stati spediti. Dall'altra parte i diffidenti, che però erano però dibattuti. Da un verso non c'era la possibilità di dimostrare che fosse una truffa, dal momento che sul sito c'era scritto chiaramente che i primi notebook sarebbero stati spediti non prima di un mese. Fino a quella data bisognava concedere a Valdi la buona fede, anche perché 2Checkout diceva di essere soltanto un tramite e che Madison Celebrity aveva fino a quel momento le carte in regola e non c'era ragione di sospettare più del dovuto.



La pagina di Medison Celebrity che consentiva di ordinare il notebook a 150 dollari tramite il distributore 2Checkout, che ha poi fatto marcia indietro e ha restituito i soldi delle prenotazioni. Ora è scomparsa dal sito

Il popolo della rete dei diffidenti però non è stato ad aspettare ed è partita una vera e propria indagine non ufficiale su Valdi e la società, capeggiata da siti creati ad hoc come www.madisonscam.info (ancora attivo) e www.madisoncelebrity.info, non più accessibile oggi. Gli "investigatori" hanno scoperto che il sito www.madisoncelebrity.com faceva capo alla società www.medison.se, che però nei contatti riportava un indirizzo del Kent, in Inghilterra. Ma a quel indirizzo alcuni naviganti si recarono veramente, senza trovare nulla. Scoprirono e divulgarono anche gli indirizzi di Valdi (valdi@medison.se e valdi_ivancic@hotmail.com), ai quali inizialmente il manager rispondeva in maniera trasparente. Un po' alla volta però qualcosa si è incrinato nell'organizzazione di Medison Celebrity. Probabilmente tempestati di telefonate, hanno disabilitato i numeri telefonici che apparivano sul sito e anche gli indirizzi e-mail dei dipendenti e dello staff. Valdi, in un suo blog, ha anche intimato i clienti di non chiamare i numeri privati del suo staff. Gli investigatori dilettanti erano arrivati anche a questo. Non solo: qualcuno ha scoperto che la "policy" del sito era stata copiata di sana pianta da quella di Apple (www.apple.com/legal/privacy/), mentre le specifiche del computer in vendita erano state copiate, compresi errori e refusi, da un notebook proposto da Clevo. L'indirizzo era www.clevo.com.tw/products/M540V.asp, ma ora è stato rimosso. Insomma, un indizio è un indizio, due indizi sono due indizi e tre indizi sono una prova. E la prova attesa della truffa, o quantomeno dell'ingenuità di Valdi, era la mancata consegna del notebook.

:: L'epilogo

Nel frattempo un nuovo comunicato stampa di Medison prometteva la restituzione dei soldi a tutti quelli che avevano già pagato, se i notebook non fossero stati spediti in tre mesi (non più un mese, dunque). E 2Checkout, che all'inizio sosteneva che nel modo di procedere di Madison Celebrity non ravvisava irregolarità, dopo qualche settimana ha preso le distanze da Medison e poco dopo si è resa disponibile a restituire i soldi a chi aveva già pagato. E Medison Celebrity? Il prodotto in vendita a 150 dollari c'è ancora, ma se si fa clic su Buy ora dice che il loro "web shop" è in costruzione (2Checkout non ha più nulla a che fare con Medison), nelle news del sito dice che ha trovato un'altra società brasiliana disposta ad assemblare i computer, la policy di privacy è stata riscritta senza copiare quella di Apple e i numeri di telefono sono scomparsi dai contatti: "the phone lines are temporarly closed". E a oggi non sappiamo ancora se Valdi abbia tentato una truffa maldestra (non ha guadagnato nulla, visto che i soldi sono passati attraverso 2Checkout) o sia stato semplicemente un imprenditore pasticcione che ha tentato un business impossibile. La cosa bella è che in rete si possono trovare sia veri affari, sia tentativi di imbrogli o, quantomeno, occasioni impossibili. Ma anche tutte le informazioni per scoprire la verità. ■

ALDI

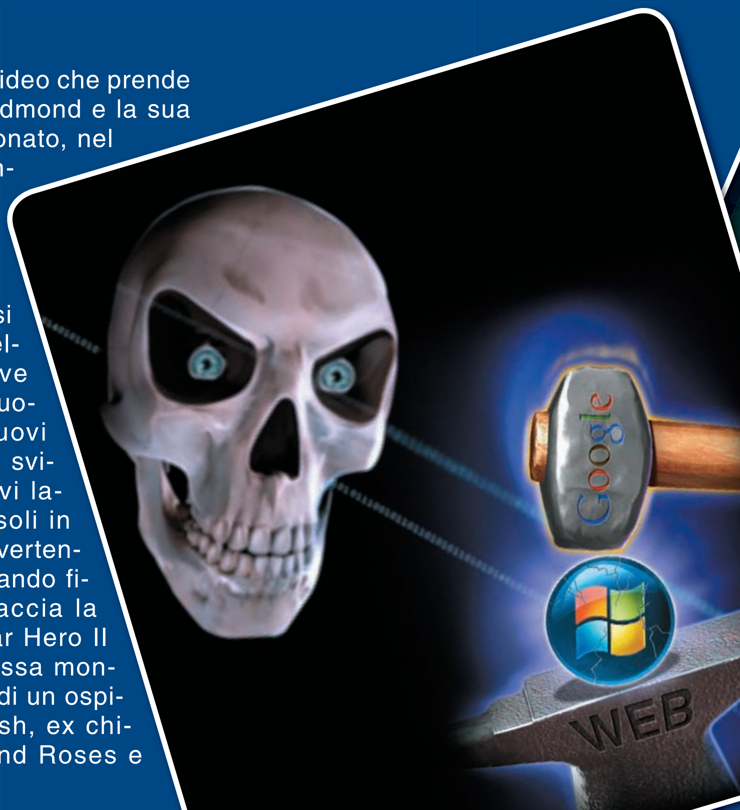
ADDIO zio Bill

Nel bene, e soprattutto nel male, è stato uno dei nomi più volte presenti sulla nostra rivista ed ora si è ufficialmente ritirato

Dobbiamo ammetterlo, ci mancherà!!! Con quella faccia un po' da sfigato, quel suo modo di fare veramente poco carismatico e quel suo continuo complesso di inferiorità (solo nelle occasioni pubbliche e non certo per il patrimonio) con il rivale/amico di sempre Steve Jobs. Beh, nelle scorse settimane si è celebrato il suo vero e proprio addio, anche se la notizia era già ufficiale, Bill Gates molla la Microsoft, o quantomeno il suo ruolo al suo interno mantenendone il controllo azionario (ci ricorda qualcosa?!?!?!). Quale occasione migliore del Ces di Las Vegas per salutare tutti... Questa manifestazione è sempre stata la vetrina per Bill e la sua società per presentare nuovi prodotti e strategie e questa volta, per l'ultima volta, Bill ha voluto parlare più che altro di se e delle strategie per il futuro della sua creatura.

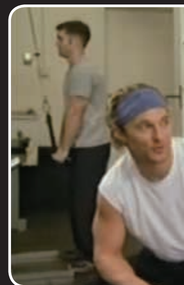
Si comincia con un video che prende in giro il Boss di Redmond e la sua futura vita da pensionato, nel video compaiono anche Hillary Clinton, Bono Vox (sigh!!!) e Russel Crowe.

Dopo questo lo Zio si protrae a parlare delle nuove prospettive del suo gruppo, le nuove partnership, i nuovi progetti in corso, gli sviluppi e quant'altro vi lasciamo trovare da soli in rete. La parte più divertente viene alla fine quando finalmente Bill imbraccia la sua Gibson di Guitar Hero II e sfida la campionessa mondiale ma con l'aiuto di un ospite d'eccezione: Slash, ex chitarrista dei Guns and Roses e









ora dei Velvet Revolver, che offre al padrone di casa un bel sostegno con la sua Les Paul vera e tonante.

Insomma Gates ha voluto lasciare in leggerezza, come crediamo che sia giusto, in fin dei conti non va a fare il monaco asceta in Tibet e neanche si ritira in miseria in qualche baracca sulla spiaggia di Santa Monica. Semplicemente si dedicherà alla Bill & Melinda Gates Fundation e, onestamente, questo giro non ce la sentiamo di prenderlo in giro più di tanto. Di sicuro ci mancherà abbiamo però delle certezze che riescono a consolarci un po':

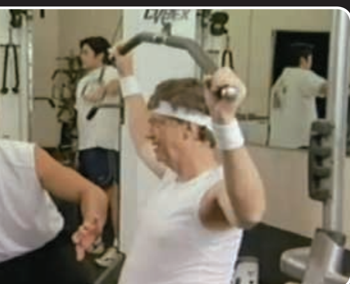
- I prodotti Microsoft continueranno a funzionare come vogliono loro e non come dovrebbero
- I sistemi operativi Windows futuri non saranno certo meglio di Vista, anche se ci vorrebbe poco
- La posizione di strapotere sul mercato e le vessazioni verso gli altri operatori continueranno
- Il sostituto di Bill sarà certamente pervaso dello stesso insipido fascino ma in compenso non avrà l'autorevolezza del vecchio squalo che aveva Gates
- Continueremo a ricercare e svelare ogni minima pecca dei prodotti di casa Redmond e questo lavoro non ci porterà via molto tempo.

Ci mancherai zio Bill... ma non così tanto!!!

BigG









Configurazione avanzata di VIRTUALBOX



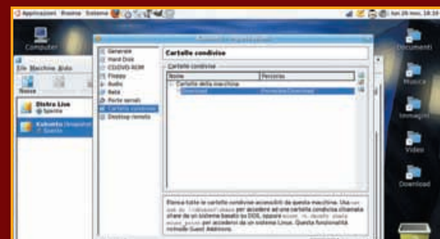
Dalle guest additions agli hard disk virtuali... tutto quello che serve per espandere le potenzialità della virtualizzazione

Virtualbox è uno dei migliori sistemi di virtualizzazione attualmente disponibili. Prestazioni e facilità d'uso sono tre le sue caratteristiche di spicco: con pochi click del mouse è possibile creare macchine virtuali per testare le versioni delle nostre distro Live Linux preferite, ad esempio; le funzionalità più avanzate, però, richiedono qualche messa a punto ulteriore.

In queste due pagine, quindi, scopriremo cosa sono ed a cosa servono le Guest Additions, fornendo poi istruzioni dettagliate per gestire al meglio le partizioni delle nostre macchine virtuali.

:: Le Guest Additions

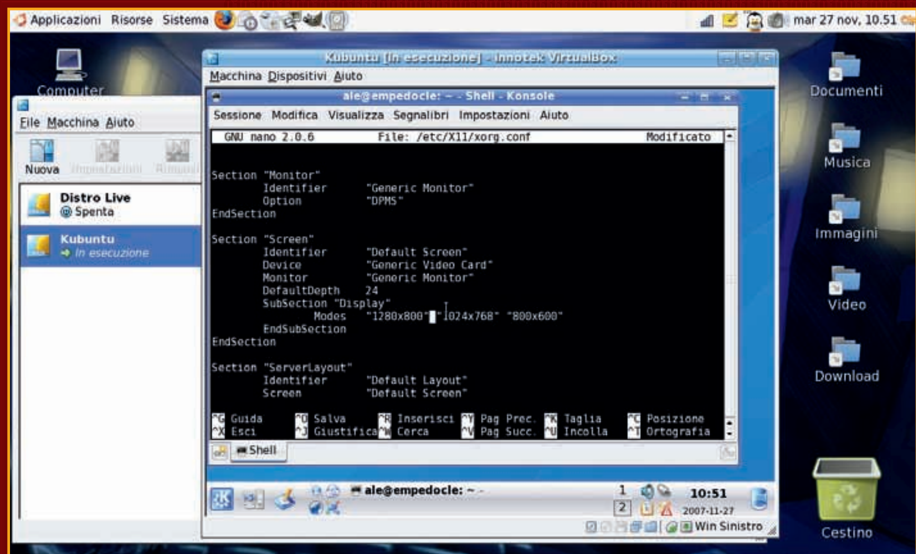
L'utilità delle normali macchine virtuali create con Virtualbox è indubbia. A volte, però, vorremmo una maggiore integrazione con il sistema host sottostante (il computer "fisico"). In questo ci vengono in aiuto le Guest Additions: si tratta di un insieme di strumenti che migliorano la comunicazione tra host e macchine virtuali, aumentando poi le prestazioni di quest'ultime grazie a driver grafici ottimizzati. Più in dettaglio, grazie alle Guest Additions potremo passare automaticamente dalla finestra di una macchina virtuale al desktop dell'host con il semplice spostamento del puntatore (senza cioè dover schiacciare il tasto Ctrl) e, cosa più importante, potremo facilmente condividere directory e clipboard tra il PC reale e le macchine guest. Vediamo dunque come procedere.



Con le Guest Additions potremo condividere cartelle tra una macchina reale ed una virtuale.

:: Precediamo con l'installazione

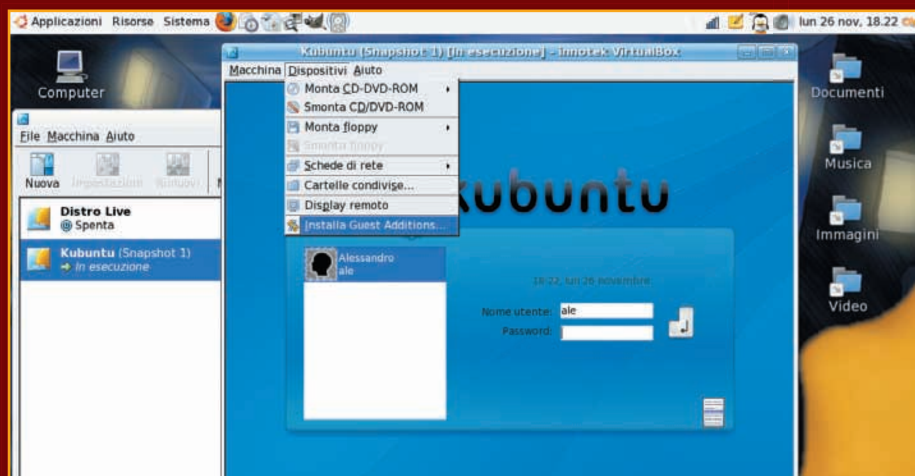
Come sistema host d'esempio andremo ad utilizzare Ubuntu 7.10, mentre il sistema virtualizzato sarà la controparte con interfaccia KDE della medesima distro, Kubuntu 7.10. Avviamo normalmente la nostra Kubuntu virtuale all'interno di Virtualbox, quindi clickiamo sul menu Dispositivi in alto nella finestra contenente la macchina virtuale; dal menu selezioniamo la voce "Installa Guest Additions". Effettuiamo il login in Kubuntu con il nostro utente principale. A questo punto apriamo una console (menu K > Sistema > Konsole), digitiamo il comando "sudo mount /dev/cdrom /media/cdrom" ed inseriamo la password del nostro utente: le Guest Additions, infatti, vengono distribuite come immagine di un CD-ROM ed è necessario montare quest'ultimo prima di procedere all'installazione delle prime. Sempre in console entriamo nella directory del CD con "cd /media/cdrom" e lanciamo da root il programma di installazione delle Guest Additions, così: "sudo ./VBoxLinuxAdditions.run". Verrà quindi installato nella macchina virtuale il driver grafico ottimizzato e sarà possibile attivare tutte le estensioni fornite dalle Guest Additions con un semplice riavvio del PC guest (se la nostra macchina virtuale utilizza Windows, invece, il click su "Installa Guest Additions" avvierà automaticamente un apposito installer).



Modifichiamo la risoluzione video della nostra macchina virtuale.

:: Configurazione avanzata

Per terminare la configurazione avanzata del desktop virtuale, quindi, non ci resta che scegliere una risoluzione adatta per il server X di Kubuntu: apriamo una console nella macchina guest e scriviamo "sudo nano /etc/X11/xorg.conf"; cerchiamo 'Section "Screen"' ed inseriamo la risoluzione da adottare nella riga dei 'Modes'.
Ad esempio, se abbiamo un monitor 1280x800 e vogliamo utilizzare la nostra macchina virtuale in modalità fullscreen facciamo diventare così la



Installiamo le Guest Additions in una Kubuntu "virtuale"...



riga: 'Modes "1280x800"'. Salviamo (Ctrl + O) ed usciamo dall'editor (Ctrl + X). Ora condividiamo una directory. Nella finestra della macchina virtuale clickiamo su "Dispositivi" e selezioniamo "Cartelle condivise". Premiamo "Ins" sulla tastiera e, nella finestra che appare, scegliamo la directory da condividere (Percorso cartella) ed il nome da attribuire a questa directory nella macchina virtuale (Nome cartella). Assicuriamoci che l'opzione "Rendi permanente" sia attiva.

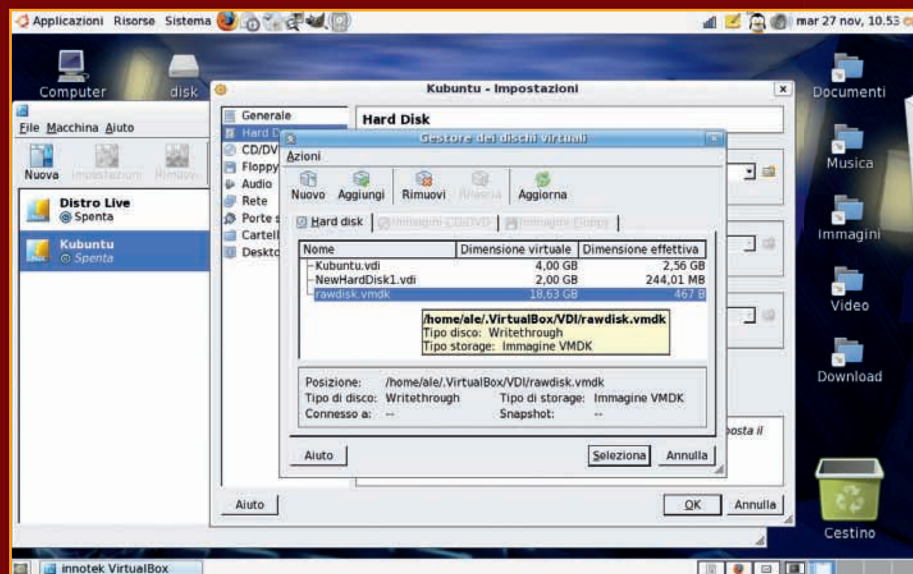


:: Accesso alle cartelle condivise

A questo punto, per avere accesso alla nostra cartella condivisa apriamo una console nella macchina virtuale e creiamo una directory apposita, ad esempio /mnt/host. Quindi montiamo lì la directory condivisa: "sudo mount -t vboxsf cartella /mnt/host". L'opzione -t è seguita dal file system che gestisce le cartelle virtuali (vboxsf), quindi nella linea inserita abbiamo il Nome della cartella ed infine la directory dove effettuare il mount. Se la nostra macchina guest utilizza Windows, invece, per avere accesso ad una cartella condivisa clickiamo su Start > Esegui e lanciamo "net use x: \\vboxsvr\cartella"; 'x' indica che la directory sarà raggiungibile mediante il drive 'x' mentre 'cartella' è il nome della cartella condivisa.

:: Dischi fisici in Virtualbox

Per aumentare le prestazioni delle nostre macchine guest è possibile utilizzare un accesso diretto alle partizioni invece che i più lenti dischi virtuali. Ad esempio, possiamo dedicare un secondo hard disk interamente a Virtualbox. Vediamo come procedere. Apriamo una console nella macchina host, entriamo nella directory con le immagini dei dischi ("cd ~/.VirtualBox/VDI") e creiamo un disco 'raw' con il comando seguente: "sudo VBoxManage internalcommands createrawvmdk -filename rawdisk.vmdk -rawdisk /dev/hdb -register". Il parametro -rawdisk indica il dispositivo del nostro secondo hard disk (/dev/hdb) mentre -filename è seguito dal file che punta al dispositivo (rawdisk.vmdk). Per accedere dall'utente normale a rawdisk.vmdk modifichiamo il proprietario del file ("sudo chown utente:utente rawdisk.vmdk"). Nel caso di host Windows, il dispositivo da dare in pasto al parametro -rawdisk è del tipo \\.\PhysicalDrive0. Creato il file rawdisk.vmdk, potremo utilizzare il nostro disco come se si trattasse di un normale hard disk virtuale di Virtualbox.





I dischi fisici vengono visti da Virtualbox come normali hard disk virtuali.

Privacy alla AMERICANA

Quanto possono spingersi in là le forze dell'ordine per garantire ordine e rispetto delle leggi??? Negli USA molto!!!

La cosa no giunge nuova a nessuno e mille volte lo abbiamo visto nei telefilm americani, il ricercato rischia di scappare e non si ha il tempo di aspettare il giudice per il mandato e allora si procede senza facendo il possibile per assicurare il cattivo alla giustizia... Ma un conto è un telefilm, un conto la realtà... o forse no?!?!? A quanto pare la gestioni delle intercettazioni da parte dell'FBI è quantomeno "creativa", questo secondo la Electronic Frontier Foundation (EFF) che ha inoltrato al giudice circa 600 pagine di denuncia contro il Bureau per abuso di intercettazione. Da quello che sta emergendo durante il procedimento penale sembra che il procedere senza autorizzazione del giudice sia ormai una prassi resa ulteriormente facile dalle tecnologie sempre più sofisticate, quindi l'agente che deve procedere a intercettare qualcuno va dal tecnico e gli dice di farlo anche senza un mandato, se il tecnico si rifiutasse sarebbe spesso scavalcato da altri più "collaborativi"...



Secondo la direzione dell'FBI gli agenti sono abituati a lavorare nelle pieghe della legge al fine di poter procedere con le indagini ma, in nessun caso, agiscono contro la legge stessa, sarà anche così ma a noi restano dei dubbi in proposito...

Secondo l'EFF invece da anni gli agenti si spingono ben oltre i regolamenti interni e la legge stessa.

Su tutto questo si stende poi l'approvazione della legge Protect America Act, ora sostituito dal Restore Act, un po' più garantisca ma comunque in grado di scavalcare alcuni dei diritti imprescindibili di qualcuno.

Sappiamo benissimo quanto sia importante poter dar la caccia a malavitosi, terroristi e quant'altro e quanto sia difficile agire all'interno della legge quando il tuo avversario ne agisce al di fuori ma la grande paura è che si arrivi a giustificare tutto con questo procedimento, poco tempo fa abbiamo parlato di cosa sta succedendo nel Regno Unito, negli USA la situazione è già molto più grave e consolidata, tra un po' ci sarà veramente da stare attenti che per proteggerci non finiscano per chiuderci tutti in delle stanzette buie perché ognuno di noi potrebbe fare del male a qualcunaltro...

Occhi aperti, sempre!!!

BigG

Java, HACK ovunque!

Con Java mobile possiamo addentrarci nella programmazione di tutto, soprattutto i nostri cellulari.



Java, chi non lo conosce? Chi non ha mai caricato qualche giochino sul proprio cellulare? chi non è mai stato infastidito da martellanti pubblicità di suonerie, sfondi, animazioni e (dulcis in fundo), i famosi "giochi giava" ?

Questo articolo è dedicato alla piattaforma Java per dispositivi mobili: Java 2 Micro Edition, j2me per gli amici :-)

:: Come funziona ?

Per poter supportare al meglio tutta la vasta gamma di terminali esistenti, i progettisti di J2ME hanno deciso di dividere concettualmente tutti i tipi di terminali in diversi tipi/categorie.

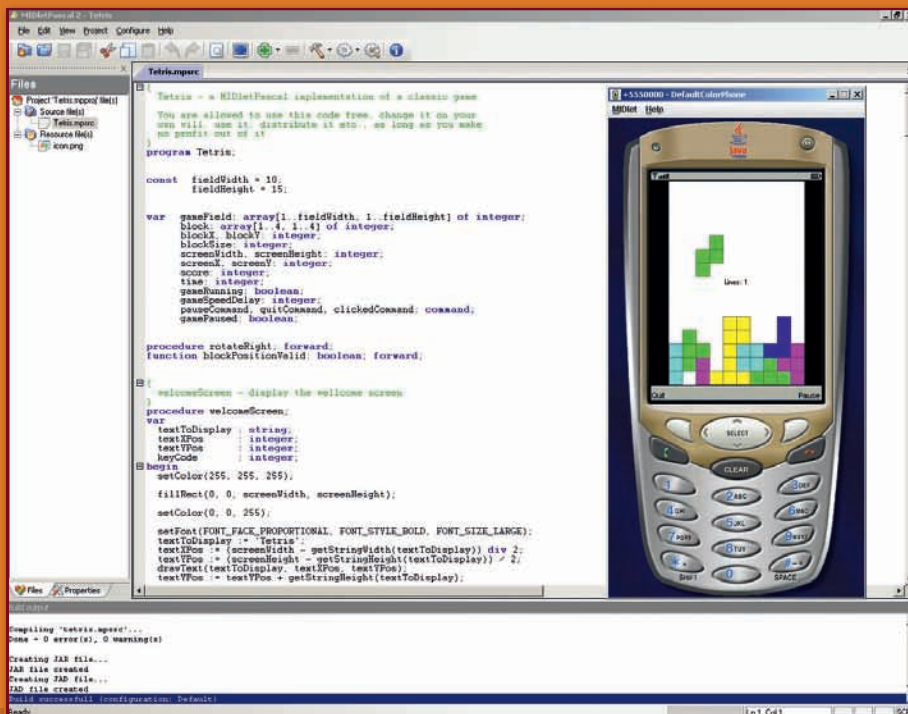
Per comprendere meglio, immaginiamo la struttura del sistema applicativo di un cellulare come un sistema a strati.

Allo strato più basso c'è la ferraglia: parti metalliche, tastierino, schermo.

Quindi c'è il sistema operativo (che può essere il famoso Symbian, Windows Mobile o un sistema operativo ad hoc sviluppato dalla casa produttrice del terminale).

Poi c'è la macchina virtuale Java, ovvero quella che interpreta il codice delle nostre midlet (così si chiamano i programmi scritti in J2ME). Questo tipo di macchina virtuale viene denominata KVM (Kylobyte Virtual Machine), data l'esigua dimnsione).

Questi 3 livelli sono comuni a tutti i terminali, adesso cominciano le differenziazioni: arrivati a questo punto, i tipi di dispositivi si dividono in due "configurazioni": CDC e CLDC. In parole povere CDC è per i dispositivi più potenti e con connessione di rete continua (a volte anche a banda larga), mentre CLDC è per terminali



meno potenti e con connettività limitata (cellulari ad esempio).
Detto questo, ogni configurazione ha i suoi "profili", ovvero set di classi predefinite. CDC ha 3 profili: Fountation Profile, Personal Basis Profile , Personal Profile. CLDL ha invece i più conosciuto e blasonato MIDP.
CDC/CLDC , MIDP

:: Bello!

Si, Java mobile è molto bello. J2me è lo standard de facto per applicazioni mobili dato che non c'è telefono (abbastanza moderno) che non abbia un'interprete Java.



Per forza di cose, J2ME è profondamente diverso dal fratello maggiore J2SE (Java 2 Standard Edition, la versione di Java per i computer). Ovviamente non ci sono né Swing né AWT, il package java.net è fortemente ridotto e funziona anche diversamente (sia dal lato concettuale che dal lato pratico). A differenza di J2SE, in J2ME socket, connessioni con l'esterno ed in generale il networking sono gestiti quasi interamente da un'unica "entità", il Generic Connection Framework: un set di classi che permette di gestire connessioni tramite socket pure, protocollo HTTP, datagrammi UDP e altro.
La parte grafica è gestita tramite un set di classi concettualmente diverse dai classici set Swing/AWT. Non ha senso parlare JFrame, JPanel e JMenuBar: quasi tutto viene gestito tramite le classi Form, Display che rappresentuano concettualmente rispettivamente l'interfaccia grafica (i bottoncini, le aree ti testo e i radio button che vediamo sullo schermo del telefonino) e il display fisico del cellulare.

Dato che non ci sono SWING e AWT, non ci sono neanche i comuni metodi actionPerformed() et similia, tuttavia qualcosa di molto simile è stato utilizzato per gestire i comandi. L'interfaccia CommandListener e il metodo commandAction() offrono tutto il necessario per gestire una semplice interfaccia grafica.Ad ogni modo, J2ME non è solo questo.

:: Reti

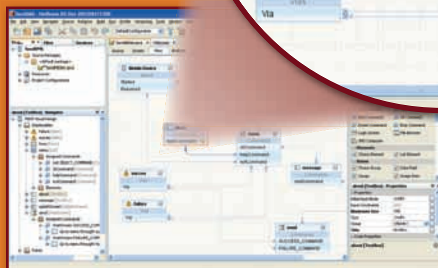
Essendo Java un linguaggio con un ottimo supporto alle reti, non poteva mancare in J2ME un altrettanto buono anche se ristretto dato l'ambiente supporto alle comunicazioni via rete.

La gestione delle comunicazioni viene gestita attraverso il Generic Connection Framework. Questo framework è un set di una decina di classi e qualche interfaccia che consentono di gestire la maggior parte dei metodi di comunicazione.

Tutto si basa sulla classe Connector e suo suo metodo open(String) . Questo metodo prende come argomento una (talvolta anche più d'una) stringa che indica il tipo di risorsa da richiedere.

Ottenuta la connessione, che può essere una connessione HTTP, Socket o datagramma UDP, i metodi getInputStream() e getOutputStream() ci forniscono il necessario per leggere e scrivere nella comunicazione. Ovviamente, in base al tipo di connessione cambiano i metodi, ma questa è una cosa ovvia :-).





PACCHETTI AGGIUNTIVI

Per essere standard, la definizione standard di Java mobile definisce un set abbastanza ristretto di funzionalità.
Proprio per la diversità di terminali disponibili, molti produttori hanno da tempo messo a disposizione pacchetti opzionali per lo sviluppo in J2ME. Un esempio? i pacchetti per l'utilizzo del BlueTooth, quelli per l'accesso al filesystem del dispositivo o quelli per l'utilizzo delle capacità multimediali del dispositivo.
Questo è un gran vantaggio perchè mette a disposizione funzionalità avanzatissime, ma spesso crea incompatibilità tra i dispositivi (ad esempio una marca di cellulari ha un buon supporto per il networking via bluetooth in Java, mente un'altra marca non lo ha e di conseguenza la midlet funzionerà bene sui cellulari della prima marca e non funzionaerà proprio sul cellulari della seconda)

:: Conclusioni

J2ME è una tecnologia splendida, che ci può essere utile in un sacco di casi.
Sebbene possa sembrare una cosa stupida, con J2ME sono stati creati anche tool relativamente famosi: il conosciutissimo Bloover (tool di analisi della sicurezza dei cellulari), creato dal gruppo di http://trifinite.org è scritto proprio in J2ME.
Non è difficile Programmare qualcosa di simile. ■



QUATTORD. ANNO 8 - N°143 - 25 GENNAIO / 7 FEBBRAIO 2008 - €2,00
80143
9 771594 577001
WLF PUBLISHING